STND-20081107A

STATEWIDE INFORMATION SECURITY STANDARD

Information Security
Identification and Authentication

Draft

Office of the Chief Information Officer

Department of Administration
Information Technology Services Division
PO Box 200113
Helena, MT 59620-0113
Tel: (406) 444-2700
FAX: (406) 444-2701

<Date Published>

Brian Schweitzer
Governor

State of Montana

DEPARTMENT OF ADMINISTRATION
Janet R. Kelly, Director

CHIEF INFORMATION OFFICER
Richard B. Clark

DRAFT STATEWIDE STANDARD: INFORMATION SECURITY IDENTIFICATION AND AUTHENTICATION

EFFECTIVE DATE: DECEMBER 1, 2010
APPROVED: <DATE APPROVED>

I. Purpose

This **Information Security Identification and Authentication Standard** (Standard) establishes the specifications and process requirements to implement the **Statewide Policy: Information Security Identification and Authentication** (Policy) for computer and information systems security.

II. Authority

This instrument has been developed by the Office of the Chief Information Officer of the State of Montana to further the statutory responsibilities under §2-17-534 MCA. Security responsibilities of department, as delegated by the Director, Department of Administration.

The State of Montana Chief Information Officer is responsible for developing policies, standards and guidelines, including minimum requirements, for providing adequate information security for agency operations and assets. This Standard is consistent with the requirements of the Montana Information Technology Act for securing information technology and §2-15-114 MCA. Security responsibilities of departments for data.

This Standard has been prepared for use by State agencies. It may also be used by nongovernmental organizations on a voluntary basis and is not subject to copyright. Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on agencies under statutory authority. Nor should this Standard be interpreted as altering or superseding the existing authorities of the department directors or any other State official.

This Standard may conflict with other instruments currently in effect. Where conflicts exist, the more restrictive instrument governs. The development of future policies or standards will explicitly identify and retire any superseded portions of current policies or standards.

III. Applicability

This standard is applicable to parties subject to the **Statewide Policy: Information Security Identification and Authentication.**

IV. Scope

The Standard specifies and requires the implementation of a computer security identification and authentication controls for the information systems and assets managed or controlled by each agency.

This Standard encompasses security identification and authentication for information systems (IS) for which agencies have administrative or statutory responsibility, including systems managed or hosted by third-parties on behalf of agencies.

This Standard may conflict with other information system (IS) standards currently in effect. Where conflicts exist, the more restrictive instrument has take precedence. The development of future policies or standards will explicitly identify and retire any superseded portions of current policies or standards.

V. Definitions

Agency	Any entity of the executive branch, including the university system. Reference §2-17-506(8), MCA.
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. Reference 44 U.S.C., Sec. 3542.
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Reference 44 U.S.C. Sec. 3502.
Information Resources	Information and related resources, such as personnel, equipment, funds, and information technology. Reference 44 U.S.C. Sec. 3502.
Information Technology	Hardware, software, and associated services and infrastructure used to store or transmit information in any form, including voice, video, and electronic data. Reference §2-17-506(7), MCA.

Refer to the Statewide Information system Policies and Standards Glossary for a list of local definitions.

Refer to the National Information Assurance (IA) Glossary, at http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf for common information systems security-related definitions.

Refer to the National Institute of Standards and Technology Special Publication 800-63 Revision 1 Electronic Authentication Guideline (NIST SP800-63), paragraph 4 for a list of identification and authentication-specific definitions.

VI. Requirements

In compliance with the **Statewide Policy: Information Security Identification and Authentication**, the requirements and specifications for this Standard are derived and adopted from the National Institute of Standards and Technology Special Publication 800-53 (NIST SP800-53) Recommended Security Controls for Federal Information Systems and Organizations (NIST SP800-53), Federal Information Processing Standard publications (FIPS PUB), and other NIST publications as specifically referenced herein.

A. Management Requirements

Each agency shall ensure that an organization structure is in place to:

1. Assign information security responsibilities.
2. Perform Identification and Authentication for information systems.
3. Allocate adequate resources to implement Identification and Authentication controls.
4. Establish and evaluate performance measures to assess implementation of this Standard and subordinate procedures.
5. Develop process(es) and procedure(s) to measure compliance with this Standard.

agency Heads: The agency head (or equivalent executive officer) has overall responsibility for providing adequate resources to support the protection of information system and communication.

Information Security Officer: The Information Security Officer (also known as the Information Systems Security Officer) may be the same individual designated by the agency head to administer the agency's security program for data under MCA 2-15-114. Security Responsibilities Of Departments For Data. Specific responsibilities under this policy are:

1. Evaluate Identification and Authentication issues within the agency and all component organizations.
2. Provide resolution recommendations to the agency head, attached agencies and division administrators, if any.
3. Develop agency policies, standards, and procedures as required.

B. Performance Requirements

Each agency shall develop and implement Identification and Authentication security controls based on an evaluation of information systems using the NIST ***risk management framework*** that:

1. Uses the categorization standards of:
    a. Federal Information Processing Standards Publication (FIPS PUB) 200 Minimum Security Requirements for Federal Information and Information Systems

b. Federal Information Processing Standards Publication (FIPS PUB) 199 Standards for Security Categorization of Federal Information and Information Systems

2. Uses guidance provided by:

   a. The agency follows the Executive Office of the President, Office of Management and Budget Memorandum E-Authentication Guidance for Federal Agencies (OMB 04-04) Attachment A, *Attachment A - E-Authentication Guidance for Federal Agencies*, as guidance for electronic authentication under the Standard:

      i. Assurance Levels and Risk Assessments

      ii. E-Authentication Process

      iii. Use of Anonymous Credentials

      iv. Technology Requirements

   b. NIST SP800-63 Revision 1 Electronic Authentication Guideline

   c. FIPS PUB 201-1 Personal Identity Verification (PIV) of Federal Employees and Contractors.

   d. FIPS PUB 190 Guideline For The Use Of Advanced Authentication Technology Alternatives

   e. NIST SP800-6 Guide for Mapping Types of Information and Information Systems to Security Categories

3. Provides additional service: The organization performs additional security-related functions as required by Identification and Authentication measures, including distributing security advisories, performing vulnerability assessments, educating users on security, and recommending security solutions consistent with common controls.

4. Implements specified levels of Identification and Authentication Standard(s) and controls, based upon the following requirements:

   a. As determined by completion of the risk management process specified in and based upon NIST SP800-39 Managing Risk from Information Systems – An Organizational Perspective. After review of the risk assessment(s), agency management shall determine any changes in the level of process, standards and controls.

   Or,

   b. Implement the **lowest** level of Identification and Authentication Standard(s) and controls based upon NIST SP800-53 Recommended Security Controls for Federal Information Systems, Annex 1, Low-Impact Baseline

Identification and Authentication (IA) family (**Annex 1**) not later than **December 1, 2010.**

5. Implements this Standard(s) through procedure(s).
6. Reviews Identification and Authentication controls and process and procedure(s) annually, and implement authorized changes to policy, standard(s), or procedure(s).
7. Is based upon the latest publicly available versions of publications referenced within this Standard *at the date of approval* of this Standard. (Note: Because newer versions of the publications referenced herein become available from time-to-time, each agency is encouraged to stay current by using the most recent versions, as deemed feasible by each agency. Future revisions of this Standard shall reference then currently-available versions.)

VII. Compliance

Compliance with this Standard shall be evidenced by adherence to the requirements specified above, as described in the referenced publications.

VIII. Standard Changes and Exceptions

Standard changes or exceptions are governed by the Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards. Requests for a review or change to this instrument are made by submitting an Action Request form (at http://itsd.mt.gov/policy/policies/action_request.doc). Requests for exceptions are made by submitting an Exception Request form (at http://itsd.mt.gov/policy/policies/exception_request.doc). Changes to policies and standards will be prioritized and acted upon based on impact and need.

IX. Closing

Direct questions or comments about this instrument to the State of Montana Chief Information Officer at ITSD Service Desk (at http://servicedesk.mt.gov/ess.do), or:

PO Box 200113
Helena, MT 59620-0113
(406) 444-2700
FAX: (406) 444-2701

X. References

A. Legislation

- §2-15-114 MCA – Security Responsibilities of Departments for Data.
- §2-17-534 MCA - Security Responsibilities of Department.

B. Policies, Directives, Regulations, Rules, Procedures, Memoranda

- MOM 3-0130 Discipline
- State of Montana Continuity of Government plans, policies, standards, and procedures (future)
- Office of Management and Budget Memorandum E-Authentication Guidance for Federal Agencies (OMB 04-04)
- Statewide Policy: Establishing and Implementing Statewide Information Technology Policies and Standards
- Statewide Procedure: Establishing and Implementing Statewide Information Technology Policies and Standards

C. Standards, Guidelines

- Guide To NIST Information Security Documents
- NIST SP800-53 Recommended Security Controls for Federal Information Systems
- NIST SP800-53 Recommended Security Controls for Federal Information Systems, Annex 1, Low-Impact Baseline Identification and Authentication (IA) family (Annex 1)
- NIST SP800-53 Recommended Security Controls for Federal Information Systems, Annex 2, Moderate-Impact Baseline Identification and Authentication (IA) family
- NIST SP800-53 Recommended Security Controls for Federal Information Systems, Annex 3, High-Impact Baseline Identification and Authentication (IA) family
- NIST SP800-39 Managing Risk from Information Systems – An Organizational Perspective
- NIST SP800-63 Revision 1 Electronic Authentication Guideline
- FIPS PUB 140-2 Security Requirements For Cryptographic Modules
- FIPS PUB 199 Standards for Security Categorization of Federal Information and Information Systems
- FIPS PUB 201-1 Personal Identity Verification (PIV) of Federal Employees and Contractors.
- FIPS PUB 200 Minimum Security Requirements for Federal Information and Information Systems

- FIPS PUB 190 Guideline For The Use Of Advanced Authentication Technology Alternatives
- NIST SP800-60, Latest Revision, Guide for Mapping Types of Information and Information Systems to Security Categories

XI. Administrative Use

Product ID:	STND-20081107a
Proponent:	Chief Information Officer
Publisher	Office of the Chief Information Officer
Published Date:	<Date Published>
Version:	0.6.28
Version Date:	3/9/2009
Custodian:	Policy Manager
Approved Date:	<Date Approved>
Effective Date:	December 1, 2010
RIM Class:	Record
Disposition Instructions:	Retain for Record
Change & Review Contact:	ITSD Service Desk (at http://servicedesk.mt.gov/ess.do)
Review:	Event Review: Any event affecting this instrument may initiate a review. Such events may include a change in statute, key staff changes or a request for review or change.
Scheduled Review Date:	December 1, 2015
Last Review/Revision:	<None>
Changes:	